Hastings Communications and Entertainment Law Journal

Volume 19 | Number 3 Article 3

1-1-1997

Privacy and the Internet

Maureen S. Dorney

Privacy and the Internet†

by
MAUREEN S. DORNEY*

Table of Contents

---

† An earlier version of this Article was presented at the *Hastings Communications and Entertainment Law Journal*'s Ninth Annual Computer Law Symposium, University of California, Hastings College of the Law, February 1, 1997.

* J.D., Boalt Hall School of Law, University of California, Berkeley, 1990; B.A., University of California, Berkeley, 1979. The author gratefully acknowledges the assistance of Bruce Sinift with the research for this article.

Introduction

The increasing power of computer and telecommunications technology makes it possible to accumulate, store, manipulate, and access detailed information about individuals. With the advent of the Internet, companies are now able to record and track detailed information concerning visits to their World Wide Web sites by individuals, such as the user's e-mail address, the parts of the site visited, and material which is downloaded. As a result of these and similar developments, individuals are becoming increasingly concerned with privacy issues. A 1993 public opinion survey found that 83% of Americans are concerned with threats to personal privacy.[1] This result reflects a five point increase over the response to a poll from the previous year, and a 49-point increase from a similar survey conducted in 1970.[2] In 1996, a large public outcry arose over a database containing personal information that is provided by LEXIS-NEXIS, Inc. This controversy prompted several members of Congress to call for increased privacy protections for data related to an individual's use of the Internet.[3]

The concept of "privacy" is very broad. In the context of electronic commerce and the Internet, privacy concerns focus on the right to control the type of information about an individual or household that can be gathered and how such information can be used or disclosed to others. These concerns relate to both the disclosure of particular information and to the misuse of information. For example, misuse of data would occur if an insurance company used a record of pharmaceutical purchases to disqualify someone for insurance. Under such circumstances, the sales data on the pharmaceuticals would have been used for purposes not intended when the data was originally disclosed. Such concerns have led to questions concerning how marketers and on-line vendors can use information gathered from users either directly (*e.g.*, through a registration process) or indirectly (*e.g.*, through a "clickstream").[4]

---

1. PRIVACY AND THE NII, SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION, UNITED STATES DEP'T OF COMMERCE, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMIN. (Oct. 1995)[hereinafter PRIVACY AND THE NII].

2. *Id.*

3. Laurie J. Flynn, *Lexis-Nexis Flap Prompts Push for Privacy Rights*, N.Y. TIMES CYBERTIMES (Oct. 13, 1996)<http://search.nytimes.com/web/docsroot/library/cyber/week/1013nexis.html>.

4. A "clickstream" has been defined as the database created by the date-stamped and time-stamped, coded/interpreted, button-pushing events enacted by users of interactive

In addition, the advent of "cookies" technology has also raised privacy concerns. A "cookie" is information about the user of a web site that a web server stores in the user's web browser. Such information can include user preference or interests as indicated by the items accessed by the user during previous visits to the Web Site.[5] Other privacy issues include how consumers of products offered for sale on the Internet can ensure that sensitive payment information is protected, and the scope of privacy of electronic mail ("e-mail"). While some companies have focused on avoiding regulation of the use of such information, many on-line vendors, as well as consumers and end users, acknowledge that if these concerns are not adequately addressed, the promise of the new global market will not be realized because consumers may be less willing to embrace electronic commerce.[6]

The failure to consider these issues may also result in difficulties in conducting business with foreign companies or individuals. Many European countries have a much more comprehensive and restrictive approach to privacy issues than does the United States. By contrast, the regulation of individual privacy in the United States is governed by a patchwork of federal and state laws. The European Union has enacted a directive on privacy which establishes new European-wide standards for the gathering, use, and disclosure of personal information. Specifically, this directive prohibits the disclosure of personal information to countries without laws providing adequate protection for such data. The global nature of the Internet means that merchants located in the United States who wish to sell products and services internationally must comply with these restrictions. For example, Citibank agreed to observe the standards of German privacy law in processing credit card applications in the United States for German citizens.[7] In addition, the less comprehensive United States law relating to privacy may result in the imposition of restrictions on

---

media controlling the systems via alphanumeric PC keyboards, mice, and similar devices. *See* Coalition for Advertising Supported Information and Entertainment, *CASIE Guiding Principles of Interactive Media Audience Measurement* (last modified Oct. 9, 1996)<http://www.commercepark.com/AAAA/bc/casie/guide.html>.

5. Federal Trace Commission Staff Report, *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, at II.A.2 (Dec. 1996)<http://www.ftc.gov/www/bcp/online/pubs/privacy/privacy.htm>.

6. *See generally id.*

7. Peter Gumbel, *High Tech Zaps German Privacy Laws*, WALL ST. J., Jan. 5, 1996, at A6.

the transfer of personal data from the European Union countries to the United States.

This article will provide an overview of the various United States statutes and regulations governing privacy issues, the European initiatives which may affect how American companies approach these issues, as well as privacy proposals made by government agencies and trade associations. This article will also address how, in the absence of an overarching regulatory framework, consumers and industry have taken steps to deal with these privacy concerns, including steps taken through recently enacted or pending legislation. This article will also briefly examine recent legislation that has been introduced in Congress to address consumers' privacy concerns.[8]

I
Overview of the Right to Privacy in the United States

The United States has no comprehensive legal framework addressing privacy issues. Although the right to privacy is not expressly provided for in the United States Constitution, the courts have used the label "privacy" for certain fundamental personal rights that are inferred from the Bill of Rights.[9] Privacy is also protected in the United States by a patchwork of state and federal statutes and regulations governing the collection, use, and distribution of certain types of information by the government or by private parties. The common law recognizes the tort of "invasion of privacy" under a number of different scenarios, such as the public disclosure of embarrassing private facts. Given the number and scope of these many different laws, the regulation of privacy in relation to the use of the Internet is not consistent or easy to understand.

II
Privacy Guaranties in the Federal Constitution

Although the right of privacy is not expressly mentioned in the Constitution, the United States Supreme Court has long recognized a guarantee of certain areas or zones of personal privacy under the Constitution. The Court finds these privacy rights in the "penumbras"

8. Although the current debate over the United States Government's regulation of the export of encryption technology has significant privacy implications, that topic is beyond the scope of this article.

9. *See infra* Part II.

of specific rights included in the Bill of Rights.[10] Privacy rights grounded in the Constitution protect individuals against impositions by the government. For example, the government may not intrude upon an individual's decision to marry, procreate, or use contraceptives.[11] In determining whether a specific privacy right is protected by the Constitution, the courts balance the government's need for a specific intrusion of privacy against the strength of the privacy right at issue. The Constitution, however, applies primarily to the government and does not generally restrict the use of information by private parties.

III
Tort Law Privacy

While Constitutional privacy protects against acts by the government, privacy rights arising from tort law typically protect against the conduct of private parties.[12] The right to be free of an "invasion of privacy" under tort law originated more than a century ago, in a famous law review article authored by Professor Samuel D. Warren and future Supreme Court Justice Lois D. Brandeis.[13] Privacy was defined as the right to be left alone.[14] The authors suggested that the law should protect a zone of privacy in each person's life from the unauthorized public disclosure of private facts.[15]

Since the publication of that article, courts have developed common law torts to protect against different types of invasions of privacy.[16] The tort of invasion of privacy is generally divided into four separate categories: (1) intrusion upon one's seclusion; (2) the public disclosure of private facts; (3) publicity that places one in a false light; and (4) the misappropriation of one's name and likeness for commercial purposes.[17] Courts in most states recognize at least one of

10. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965). Justice Douglas stated that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy." *Id.* (citation omitted).

11. *See* Loving v. Virginia, 388 U.S. 1, 12 (1967); *Griswold*, 381 U.S. at 486.

12. *See* J. THOMAS MCCARTHY, RIGHTS OF PUBLICITY & PRIVACY § 5.7, at 4-59 (1995).

13. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

14. *Id.* at 195.

15. *Id.* at 215.

16. *See generally* MCCARTHY, *supra* note 12, at §§ 1.4-1.5 (examining development of the common law right to privacy).

17. William Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

these privacy rights, and many states have codified one or more privacy rights in civil or criminal statutes.[18] Thus, conduct giving rise to tort liability under the judicially developed common law may also result in liability under federal or state statutes.

Privacy torts evolved largely in response to advertising and news reporting cases.[19] Just as traditional non-electronic commerce has sometimes impinged upon these rights, so "advertising" and other news reporting in the electronic world will be subject to these restrictions. Moreover, the increasing ability to gather, use, and disclose information in the electronic world may lead to new "rights" based on these traditional tort theories.

A. Intrusion Upon Seclusion

The right of seclusion protects an individual against the unauthorized gathering of personal information. This form of privacy is invaded by the intentional intrusion "upon the solitude or seclusion of another or his private affairs."[20] To qualify as an intrusion, the conduct must be highly offensive to the reasonable person, and the personal information must not be voluntarily disclosed to the public.[21] For example, telephone wiretaps have been held to violate these rights.[22] In the context of the Internet, the process of gathering the information itself must be highly objectionable to constitute a tort based on this theory. For example, secretly collecting highly sensitive personal information about individuals on the Internet without their consent may result in damages under this theory.[23] Such conduct may also be a violation of the federal Electronic Communications Privacy Act, which, as discussed below, limits unauthorized access to communications and information systems.[24]

---

18. *See, e.g.*, CAL. CIV. CODE § 3344 (West Supp. 1997); N.Y. CIV. RIGHTS LAW §§ 50, 51 (McKinney 1992 & Supp. 1997)(recognizing only the misappropriation claim).

19. *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM L.J. 195, 222 (1992).

20. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

21. *Id.* at cmts. c, d.

22. *See* HENRY H. PERRIT, JR., LAW AND THE INFORMATION SUPERHIGHWAY § 3.5, at 93 (citing Rhodes v. Graham, 37 S.W.2d 46 (Ky. 1931)).

23. *See infra* note 41 and accompanying text. *See also infra* notes 109-113 and accompanying text (discussing attempt by LEXIS-NEXIS to provide a for-profit on-line service disclosing "personal" information).

24. *See infra* Part IV.A.

B. Public Disclosure of Private Facts

The public disclosure of private facts tort prohibits certain uses of personal information regardless of how the information is gathered. An individual's privacy rights are violated under this theory when an ordinary person would find disclosure to be highly offensive.[25] Constitutional protection of free expression under the First Amendment, however, restricts the scope of this privacy right when the facts disclosed involve a public figure or a legitimate public concern.[26] A recent example of this tort was a dispute between the illegitimate son of comedian Eddie Murphy and the *National Enquirer*.[27] The child's mother sued the *National Enquirer* about a story that revealed his relationship with Eddie Murphy and the amount of his financial support.[28] The information was not publicly known and did not appear to be a matter of public interest. The publishing of highly offensive or private information over the Internet (if not protected under the First Amendment), could result in a finding of liability under the public disclosure tort. It should be noted that this tort category encompasses the same kind of conduct regulated by the federal Privacy Act[29] and by the Fair Credit Reporting Act.[30]

C. False Light Privacy

The privacy right protected under this theory is the right to be secure from publicity that places an individual in a false light. This tort prohibits an objectionable false representation which does not meet the definition of defamation,[31] and which must have been made to the general public.[32] This form of privacy may be implicated in electronic commerce if the information disclosed concerning an individual is inaccurate or misleading, or if the custodian of computer data fails to take appropriate action to ensure the accuracy of data. Such conduct is

25. RESTATEMENT (SECOND) OF TORTS § 652D, cmt. c (1977).

26. *See* MCCARTHY, *supra* note 12, at § 5.9[B][1].

27. *See* David G. Savage, *High Court Won't Hear Tabloid's Appeal*, L.A. TIMES, Dec. 5, 1995, at A30.

28. *Id.*

29. *See infra* Part IV.B.

30. *See infra* Part IV.F.

31. RESTATEMENT (SECOND) OF TORTS § 652E (1977).

32. *Id. See* Polin v. Dunn & Bradstreet, 768 F.2d 1204, 1206-07 (10th Cir. 1985)(holding communication to seventeen business entities did not constitute dissemination to general public).

also addressed by the federal Privacy Act,[33] and the Fair Credit Reporting Act.[34]

D. Misappropriation of Name or Likeness

While the first three categories of privacy rights protect information that is "private," the right against misappropriation of name or likeness protects against the unauthorized commercial use of a person's identity.[35] It precludes the use of any aspect of an individual's name, voice, or likeness in advertisements or for other commercial uses.[36] Although misappropriation claims often involve celebrities who contest the use of their name or photographs in an advertisement for a commercial product, non-celebrities may also assert this right.[37] This form of privacy would be implicated if an individual's name or likeness was published on the Internet for commercial purposes without his or her consent.[38]

IV
Federal Regulation of Privacy

The United States has no omnibus privacy law governing the private sector's treatment of personal information. Instead, Congress has passed various federal statutes and regulations to control the collection, use, and distribution of information in particular industries. This section will provide a summary of six federal statutes regulating the privacy of individuals vis-à-vis the use of communications, computer, and/or video equipment and networks. These statutes are: (1) the Electronic Communications Privacy Act; (2) the Privacy Act; (3) the Cable Communications Policy Act; (4) the Video Privacy Act of 1988; (5) the Telephone Consumer Protection Act of 1991; and (6) the Fair Credit Reporting Act. While not all of these statutes will have a direct bearing on electronic commerce, they suggest a

33. *See infra* Part IV.B.

34. *See* PERRIT, *supra* note 22, at 94. *See also infra* Part IV.F.

35. *See* RESTATEMENT (SECOND) OF TORTS § 652C (1977).

36. *Id.* at cmt. b. This tort has been codified by statute in many states. *See, e.g.*, CAL. CIV. CODE § 3344 (West 1996).

37. *See* MCCARTHY, *supra* note 12, at § 2.1[B].

38. Further, one may violate another person's right of publicity without using the person's name or likeness in the traditional sense. As long as a plaintiff's "identity" has been misappropriated, a cause of action will exist. *See* White v. Samsung Elecs. Am., Inc., 971 F.2d 1395, 1397-99 (9th Cir. 1992), *cert. denied*, 508 U.S. 951 (1993).

framework that could be applied to resolve the privacy issues arising in electronic commerce.

A. Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA) amended a statute passed to protect individuals against government eavesdropping on telephone conversations.[39] Enacted in 1986, the ECPA covers all forms of digital communications, including data transmissions between computers, paging devices, e-mail, and video transmissions, and prohibits unauthorized eavesdropping by all persons and businesses.[40] In addition, the ECPA prohibits unauthorized access to messages stored on a computer system as well as the interception of electronic messages in transmission.[41] The ECPA clearly applies to many situations encountered in electronic commerce.

The ECPA is a complex statute, providing varying levels of privacy protection depending on: (1) whether the communication is being transmitted or is in storage;[42] (2) whether the communication is aural or electronic (such as e-mail or data transmission);[43] and (3) the type of system (public or private) where the message is found.[44] With regard to the transmission of any voice or electronic communications, the ECPA prohibits the interception, use, or disclosure of such communications, except under limited circumstances.[45] For example, providers of communication services may assist persons authorized by law in intercepting voice communications.[46] In addition, an entity providing electronic communication services may disclose information

39. 18 U.S.C. §§ 2510-2711 (1994).

40. 18 U.S.C. § 2510.

41. LANCE ROSE, NETLAW: YOUR RIGHTS IN THE ONLINE WORLD 167-75 (1995).

42. *Compare* 18 U.S.C. § 2511(4) (setting maximum imprisonment between one and five years for intercepted communications), *with* 18 U.S.C. § 2701(b) (setting maximum imprisonment between six months and two years for unlawful access to stored communications).

43. *Compare* 18 U.S.C. § 2511(4)(b) (setting maximum punishment at one year imprisonment for interception of cellular telephone transmission), *with* 18 U.S.C. § 2511(4)(a) (setting maximum punishment at five years imprisonment for communications not covered in subsection (b)).

44. *Compare* 18 U.S.C. § 2511(4)(c) (intercepting non-encrypted transmission and transmitting it to broadcasting station or redistributing for public use is not an offense), *with* 18 U.S.C. § 2511(5)(a) (subjecting interceptors of private non-encrypted transmissions to suit by the federal government).

45. *See generally* 18 U.S.C. § 2511.

46. *Id.* § 2511(2)(a)(ii).

with the originator's consent.[47] The providers of private wire or electronic communication services (such as employers) have special rights. They may intercept, disclose, or use any communication in the normal course of employment while engaged in an activity incident to rendering the service or to protecting the providers' rights or property.[48] This exception to the general prohibition, however, does not authorize random monitoring of communications except for mechanical or service quality control checks.[49]

With regard to communications stored on media, such as magnetic tapes, computer random access memory, disks, or other magnetic or optical media, the ECPA generally prohibits a company or an individual from accessing, obtaining, altering, or disclosing such stored communications.[50] Despite this general prohibition, electronic systems operators may generally review messages that are stored on a computer system, such as messages stored in a mailbox.[51] While operators may review such messages, they may *not* intentionally divulge the contents of any communication to any third person, except to a government agency when the information appears to pertain to the commission of a crime, or with the consent of the user or addressee.[52]

Concerns regarding access to stored messages have generally arisen in the context of an employer reading an employee's e-mail. A 1993 *MacWorld* survey of 301 large and small companies revealed that one in five employers occasionally read e-mail and other computer files or listened to voice mail.[53] While the ECPA would allow a systems operator to monitor employee e-mails, prior written notice to employees that their e-mail may be monitored in the normal course of business will help to avoid employees' privacy claims. Employees have not yet prevailed in lawsuits challenging the right of employers to read employee e-mail.[54] Several of these lawsuits, however, have involved companies where the employee was informed that their employer-

47. *Id.* § 2511(3)(b)(ii).

48. *Id.* § 2511(2)(a)(i).

49. *Id.*

50. *Id.* § 2701

51. ROSE, *supra* note 41, at 168-69.

52. 18 U.S.C. § 2702.

53. Tawn Hhan, *A Lesson for Office Workers: There's No Privacy in E-Mail*, FRESNO BEE, Feb. 13, 1995, at E5.

54. *Id. Cf.* Michelle Singletary, *Loose Lips an E-Mail Hazard*, NEWSDAY, Apr. 6, 1997, at F12 ("As yet there isn't much case law on this issue.").

provided e-mail service was to be used for business purposes only, and/or that it might be monitored.

The ECPA provides for both criminal[55] and civil remedies[56] in the event of a violation. Civil suits are more common because it is unclear whether government prosecutors will be interested in disputes between systems operators, employers, and users. Appropriate relief in a civil action may include actual damages suffered by the plaintiff, profits made by the violator, and attorney's fees and costs.[57]

B. Privacy Act

Unlike the other statutes discussed in this article, the Privacy Act focuses on government conduct rather than the behavior of private entities.[58] The goal of the Privacy Act is to strike a balance between the government's need to gather and use personal information and the individual's privacy interest in controlling such information. Under the Privacy Act, federal agencies may maintain records containing only such information about an individual that is relevant to accomplish the agency's purpose.[59] Information must be maintained accurately and completely, and, if possible, must be collected directly from the individual.[60]

The Privacy Act further requires every federal agency that maintains a system of records to: (1) permit the individual to control disclosure of information in the record;[61] (2) retain records of information that is disclosed;[62] (3) permit the individual to review and have a copy of information in the record;[63] and (4) allow the individual to request an amendment to information in the record.[64] The head of any agency, however, may issue rules to exempt any system of records

55. 18 U.S.C. § 2511(4)(a).

56. *Id.* § 2520.

57. *Id.* § 2707.

58. 5 U.S.C. § 552a (1994).

59. *Id.* § 552a(e)(1).

60. *Id.* § 552a(e)(2).

61. *Id.* § 552a(b). No record may be disclosed without the written consent of the individual to whom the record pertains. This requirement is subject to numerous exceptions including, among others, disclosures made to the Bureau of Census or other statistical agencies, a person pursuant to a showing of compelling circumstance, or another government agency if the disclosure is authorized by law. *Id.*

62. *Id.* § 552a(c).

63. *Id.* § 552a(d)(1).

64. *Id.* § 552a(d). If the federal agency refuses to amend a record, the individual may seek judicial review of the decision.

within the agency from the provisions of the Privacy Act.[65] In addition, the Privacy Act exempts seven classifications of records, such as records relating to law enforcement and military promotions.[66]

C. Cable Communications Policy Act

The Cable Communications Policy Act of 1984[67] provides a potentially interesting model that could be applied to address privacy issues on the Internet. The Act requires cable television companies to provide annual notification to subscribers about how their personal information is used and disclosed, and the purposes for which it is gathered.[68] Cable operators may not use the cable system to collect or to disclose personal information about subscribers without their consent except as necessary to render cable service, detect unauthorized cable reception, or pursuant to a court order.[69] A mailing list of subscribers may be distributed provided each subscriber has an opportunity to remove his or her name from the mailing list.[70] If information about a subscriber is no longer necessary for the purpose for which it is collected, the cable operator must destroy such information.[71] The remedies available to subscribers for a violation of the Cable Communications Policy Act include actual and punitive damages and reasonable attorneys' fees.[72]

D. Video Privacy Act of 1988

The Video Privacy Act of 1988 (VPA) is a *criminal* law that regulates disclosure of information about video tape rentals.[73] Congress passed the VPA in reaction to the media's ability to obtain the list of films rented by Judge Robert Bork after he was nominated

65. *Id.* § 552a(j)-(k).

66. *Id.* § 552a(k). Exemptions include records that are investigatory material used for law enforcement purposes, information used to protect the President, statistical records, information used for eligibility for federal employment or federal service, and information used to evaluate promotion in the armed forces.

67. 47 U.S.C. § 551 (1994).

68. *Id.* § 551(a)(1)(A).

69. *Id.* § 551(c)(2).

70. *Id.* § 551(c)(2)(C).

71. *Id.* § 551(e).

72. *Id.* § 551(f).

73. 18 U.S.C. §§ 2710-2711 (1994).

to the Supreme Court.[74] The VPA prohibits the disclosure of the title, description, and subject matter of a film and other personal information, except for names and addresses, without the informed written consent of the consumer.[75] The consent provision adopts an "opt-in" approach requiring specific approval from the individual for each use.[76]

E. Telephone Consumer Protection Act of 1991

The Telephone Consumer Protection Act of 1991 (TCPA)[77] is a collection of provisions regulating unsolicited telephone calls. The TCPA restricts the use of any automatic telephone dialing system or pre-recorded voice to make calls to any emergency line, health care facility, or any pager or cellular phone where the called party is charged for the call.[78] The TCPA also outlaws any calls using a pre-recorded voice that are placed to residential telephone lines without the prior consent of the recipient.[79]

The TCPA directs the FCC to prescribe regulations to protect businesses from prerecorded, unsolicited calls and to exempt from liability certain non-commercial calls that do not adversely affect privacy rights.[80] The FCC is further permitted to establish a national database to compile a list of telephone numbers of residential subscribers who object to receiving telephone solicitations and prohibit unsolicited calls to any subscriber listed in such a database.[81] A person who has received more than one telephone call in violation of the statute within any twelve-month period may bring an action to enjoin such calls and/or recover up to $500 in damages for each violation.[82] If the problem of "spamming"[83] continues to increase on the Internet, the TCPA may serve as a model to control such practices.

---

74. *See* Bob Geske, *Protecting Our Privacy Through the Electronic Keyhole of the 90's, Businesses Are Peeping Into Our Lives as Never Before*, VIRGINIAN-PILOT & LEDGER-STAR (Norfolk, Va.), Oct. 31, 1993, at C1.

75. 18 U.S.C. § 2710(b)(2)(B).

76. *Id.* For disclosure of names and addresses, the video tape service provider must merely give the consumer an opportunity to prohibit disclosure, *i.e.* "opt-out." *Id.* § 2710(b)(2)(D)(i).

77. 47 U.S.C. § 227 (1994).

78. *Id.* § 227(b)(1)(A).

79. *Id.* § 227(b)(1)(B).

80. *Id.* § 227(b)(2).

81. *Id.* § 227(c)(3)(F).

82. *Id.* § 227(c)(5). A person may opt to collect actual monetary loss from violations of the statute if that sum is greater than the $500 per violation calculation. *Id.* § 227(c)(5)(B).

83. "Spamming" is the practice of sending unsolicited promotional e-mail.

F. The Fair Credit Reporting Act

The Fair Credit Reporting Act of 1970 (FCRA) governs the disclosure of credit reports containing personal information by consumer credit reporting agencies.[84] The FCRA provides a list of permissible purposes for which personal information about a consumer may be disclosed without the individual's consent.[85] A credit agency may furnish a credit report to establish the individual's eligibility for credit, employment, insurance, or for any other "legitimate business need."[86] Whenever credit is denied to an individual based on information furnished in a credit report, the user of the credit report must supply the name and address of the credit reporting agency to the individual.[87]

The FCRA also requires credit agencies to follow reasonable procedures to assure the accuracy of personal information.[88] Credit reporting agencies must have a procedure for investigating a dispute concerning the accuracy of information in a credit report.[89] Moreover, certain obsolete information may not be disclosed in a credit report.[90]

Recently, pursuant to the provisions of the Economic Growth and Regulatory Paperwork Reduction Act of 1996,[91] the Federal Reserve Board is required to prepare a report for Congress regarding whether additional laws are needed to protect sensitive consumer information such as social security numbers.[92]

V
Privacy Rights Under State Laws

States have also enacted laws concerning a variety of different privacy rights to control the manner in which information about an individual or household is collected, used, and disseminated to others.

---

84. 15 U.S.C. §§ 1681, 1681a-1681t (1994).

85. *Id.* § 1681b.

86. *Id.*

87. *Id.* § 1681m.

88. *Id.* § 1681e.

89. *Id.* § 1681i.

90. *Id.* § 1681c. Among these are adjudicated bankruptcies more than ten years old, paid tax liens more than seven years old, and records of arrest, indictment, or conviction of a crime that antedate a credit report by more than seven years. *Id.* § 1681c(a).

91. The Act is codified in the Omnibus Consolidated Appropriations Act, §§ 2001-2711, Pub. L. No. 104-208, 110 Stat. 3009 (to be codified at scattered sections of 12 U.S.C. and 15 U.S.C.).

92. *Id.*

For example, Article I of the California State Constitution provides that the right to privacy is included among the inalienable rights of all people.[93] Unlike the privacy rights based on the United States Constitution, the objective of this privacy right is to protect against:

> (1) "government snooping" and the secret gathering of personal information; (2) the overbroad collection and retention of unnecessary personal information by government *and business interests*; (3) the *improper use of information properly obtained for a specific purpose* . . . ; and (4) the lack of a reasonable check on the accuracy of existing record[s].[94]

The California Constitution does not preclude all intrusion into individual privacy rights, but requires that any intrusion be justified by a compelling interest.[95] Conduct that constitutes an invasion of privacy under the "compelling interest" test includes improper disclosure of university grades[96] and disclosure of employee personnel files.[97]

California also regulates the extent to which telephone and telegraph companies may use personal information. Telephone companies may not disclose calling patterns, credit or financial information, services purchased, or demographic information without a consumer's written consent.[98]

The New York Civil Rights Law also establishes various categories of privacy rights.[99] It prohibits the misappropriation of the name or likeness of an individual for commercial purposes.[100] It also limits public access to various records, such as personnel records of police officers, firefighters, and court officers,[101] and the identity of the victims of sex offenses.[102] Thus, the improper use of certain categories of personal information obtained on the Internet could violate an

---

93. CAL. CONST. art I, § 1. A California appellate court has held "all people" to include corporations or partnerships. H & M Assocs. v. El Centro, 167 Cal. Rptr. 392 (Cal. Ct. App. 1980).

94. White v. Davis, 533 P.2d 222, 234 (Cal. 1975).

95. *Id.*

96. Porten v. University of San Francisco, 134 Cal. Rptr. 839, 841-43 (Cal. Ct. App. 1976).

97. El Dorado Sav. & Loan Ass'n v. Superior Court, 235 Cal. Rptr. 303, 305 (Cal. Ct. App. 1987); Board of Trustees of Leland Stanford Jr. Univ. v. Superior Court, 174 Cal. Rptr. 160, 165 (Cal. Ct. App. 1981).

98. *See* CAL. PUB. UTIL. CODE § 2891 (West Supp. 1997).

99. N.Y. CIV. RIGHTS LAW §§ 50-52 (McKinney 1992 & Supp. 1997).

100. *Id.* § 50. Specifically, any person or corporation that uses for advertising purposes the name, portrait, or picture of any living person without obtaining written consent is guilty of a misdemeanor. *Id.*

101. *Id.* §§ 50-a, 50-d.

102. *Id.* § 50-b.

individual's rights under state law as well as under common law or federal statutory provisions.

VI
Public and Private Privacy Initiatives

The patchwork nature of the laws governing privacy rights, and the lack of clear regulations to guide companies doing business on the Internet, have made it necessary for industry and consumer groups to take action to ensure privacy is protected. Both industry and consumer groups are studying different approaches to achieve an equitable balance between privacy interests and the desire to use personal information to promote electronic commerce. The United States Government has also examined these issues. Initially, in the absence of comprehensive laws, the government merely urged private entities to implement processes for protecting customer privacy. More recently, as concern over the privacy of personal information over the Internet has grown, Congress has introduced several pieces of legislation relating to on-line privacy. This section describes some of these initiatives.

A. Industry Practice

Individual companies and trade associations have examined the privacy issues described above, and adopted measures to address customer concerns. For example, while both America Online and Compuserve disclose personal information about their subscribers in the form of customized mailing lists, both also allow individual customers to opt-out of such mailing lists.[103] "In contrast, Prodigy has a policy of not disclosing any personal information about its subscribers to third-parties."[104]

The Association of Accredited Advertising Agencies (AAAA) recently issued privacy goals for electronic commerce which aim at ensuring that: "1. marketers . . . disclose their identity; 2. marketers . . . make only 'appropriate' use of personal information; 3. Consumers . . . [are] presented with options regarding what

103. NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, PRIVACY AND THE NII, SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION app. n.34 (Oct. 23, 1995)<http://www.ntia.doc.gov/ntiahome/privwhitepaper.html>.

104. *Id.*

information they wish to reveal about themselves; and 4. consumers . . . [are given] access to their personal records."[105]

The marketers advocate an "opt-out" approach and define personal information as "non-public" information.[106] Other groups, however, such as the Electronic Privacy Information Center (EPIC), a consumer group, prefer an "opt-in" approach that requires customer consent for each use of such information.[107] EPIC believes that the AAAA's definition does not go far enough because it excludes public information that some groups view as private, such as information in a driver's license data banks.[108]

On occasion, a groundswell of consumer reaction has overtaken this debate. For example, in 1991 the Lotus Development Corporation and the Equifax Corporation planned on releasing a software program containing detailed marketing information about individuals called "Lotus Marketplace: Households."[109] This program was designed to provide small companies with the kind of marketing information usually available only to large corporations.[110] When Lotus' plans were made public, however, it received letters from approximately 30,000 people complaining that such software was too intrusive.[111] Acceding to popular sentiment, Lotus decided not to release the software.[112] While consumers were initially influential, it should be noted that Lotus eventually sold the product to another company, which released it using a more subtle approach.[113] Thus, while consumers obviously influence the marketplace, their power is somewhat limited. Consequently, Congress and other regulatory agencies are reviewing strategies for protecting privacy on the Internet, as outlined below.

One strategy calls for Internet companies to develop voluntary standards for the protection of personal data. In 1996, a group of Internet companies, along with the non-profit Electronic Frontier

105. Sally Goll Beatty, *Consumer Privacy on the Internet Goes Public*, WALL ST. J., Feb. 12, 1996, at B3.

106. *Id.*

107. *Id.*

108. *Id.*

109. ROSE, *supra* note 41, at 178-79.

110. *Id.*

111. *Id.*

112. *Id.*

113. *Id.*

Foundation, launched the "eTRUST" program.[114] Companies participating in the eTrust program will adopt one or more of three options for the use of consumer data collected through their web sites: (1) "Anonymous"—no data is collected concerning users of that web site; (2) "One-to-one Exchange"—user data is collected only for the web site owner's use; and (3) "Third Party Exchange"—data is collected and provided to third parties.[115] Members of the eTrust program may display the appropriate eTrust "trustmark" to indicate to the public how they use the consumer data gained from their Web sites.[116]

B. U.S. Government Studies/Recommendations

The Government took note of this debate and launched its own study of privacy issues in June of 1995. The Clinton Administration's National Information Infrastructure Task Force (NIITF) published *Privacy and the National Information Infrastructure: Principles For Providing and Using Personal Information*.[117] The NIITF adopted the following general principles:

> Personal information should be acquired, disclosed, and used only in ways that respect an individual's privacy.
>
> . . .
>
> Personal information should not be improperly altered or destroyed.
>
> . . .
>
> Personal information should be accurate, complete and relevant for the purpose for which it is provided and used.
>
> . . .
>
> Information users should:
>
> 1. Assess the impact on privacy when deciding whether to acquire, disclose or use personal information.
>
> . . .
>
> 2. Acquire and keep only information reasonably expected to support current or planned activities.
>
> . . .

114. Laurie J. Flynn, *Group to Monitor Web Sites For Respect Of Consumer Privacy*, N.Y. TIMES CYBERTIMES (July 16, 1996)<http://search.nytimes.com/web/docsroot/library/cyber/week/0716privacy.html>.

115. *Id. See also* eTRUST (visited Apr. 14, 1997)<http://www.etrust.org>.

116. *Id.*

117. NIITF, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION (visited June 6, 1995)<http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html>.

> Information users . . . should provide adequate, relevant information about . . . why they are collecting information; . . . what steps will be taken to protect [it]; and . . . any rights of redress.
>
> . . .
>
> Information users should use appropriate technical and managerial controls to protect the confidentiality and integrity of personal information.
>
> . . .
>
> Information users should not use personal information in ways that are incompatible with the individual's understanding of how it will be used. . . .[118]

These principles recognize that the nature of the electronic medium will shape privacy policies.

Although these principles are very general, the NIITF has worked to issue more detailed guidelines. In October of 1995, the National Telecommunication and Information Administration (NTIA) published *Privacy and the NII, Safeguarding Telecommunications-Related Personal Information*, in which it reviewed various privacy issues with regard to both the telecommunications industry and new technologies such as the Internet.[119] The NTIA proposed an approach for industry that it believes achieves a fair balance between the privacy interests of individuals and the interest of electronic merchants in using personal information for marketing efforts.[120]

The suggested NTIA approach has two fundamental elements: provider notice and customer consent.[121] Under the proposed framework, the merchant would inform its customers about what personal information it intends to collect and how such data will be used.[122] The merchant is then free to use the information for *the stated purpose* once it has obtained consent from the relevant customer.[123] Affirmative consent ("opt-in") is required only with respect to sensitive personal information, while tacit customer consent ("opt-out") is sufficient to authorize the use of all other information.[124] The

118. *Id.*
119. *See* PRIVACY AND THE NII, *supra* note 1.
120. *Id.*
121. *Id.*
122. *Id.*
123. *Id.*
124. *Id.*

NTIA, however, did not clearly define what information should be considered sensitive.

The NTIA believes that this approach gives merchants and their customers the flexibility to establish a specific level of protection for a particular marketplace transaction.[125] This flexibility was designed to ensure that the approach would not be overly burdensome on industry while assuring consumers that their privacy expectations would be respected.[126] Furthermore, so long as the minimum requirements of notice and consent are satisfied, the system would be free from excessive government regulation.

The Federal Trade Commission (FTC) has also undertaken a "Privacy Initiative" to study consumer protection in the global information infrastructure.[127] After a workshop on privacy issues held in April 1995, the FTC issued a letter in September 1995 soliciting suggestions for "voluntary privacy principles" applicable to consumers' use of the Internet. The questions raised by the FTC addressed consumer privacy expectations, merchants' obligations to protect privacy, and the ability of consumers to access and correct information. Again the goal is to avoid cumbersome regulation by facilitating the development of a set of voluntary principles to govern the use of consumer information in on-line transactions.[128]

VII
Pending United States Legislation

As public concern grew over the privacy of personal data, several bills were introduced in Congress that were designed to strengthen individual privacy rights. These bills have implications for companies conducting business on the Internet. [129]

---

125. *Id.*

126. *Id.*

127. *See generally* FTC (visited Apr. 14, 1997)<www.ftc.gov>.

128. For additional information concerning the FTC Privacy Initiative, visit the FTC Website, *id.* The FTC's most recent efforts included a workshop on Internet privacy issues. *See Privacy Fears and the Internet*, WASH. POST, June 16, 1997, at A20. During that workshop, software industry leaders agreed to take active steps to develop a common standard to protect user privacy. *See* Steve Lohr, *Rare Alliance on Privacy For Software*, N.Y. TIMES, June 12, 1997, at C1.

129. Some of the proposed statutes concerned the privacy of medical records and health care information are beyond the scope of this article. *See, e.g.*, S. 1360, 104th Cong. (1996); H.R. 3482, 104th Cong. (1996).

In 1996, Congress held hearings on the Children's Privacy Protection Parental Empowerment Act of 1996, introduced by Representative Barney Frank.[130] This legislation would create civil and criminal liability for "list brokers" who knowingly collect and distribute personal information about a child without parental consent.[131] The bill would also obligate "list brokers" to disclose to parents the source of personal information gathered concerning their child, and would prohibit using information about a child collected in the course of a contest or game designed to attract that child for commercial purposes, without first obtaining parental consent.[132]

Also in 1996, Representative Edward Markey introduced the Communications Privacy and Empowerment Act.[133] This legislation would require the FTC to hold hearings and propose changes to current regulations to protect the privacy of consumers and children in general.[134]

On January 7, 1997, Representative Bruce Vento introduced the Consumer Internet Privacy Protection Act of 1997.[135] This legislation would prohibit "interactive computer services" from disclosing personally identifiable information concerning subscribers to third parties without first obtaining the subscriber's "prior informed written consent."[136] Subscribers would also have the right to review and correct the contents of personal information maintained by the computer service and to request and obtain the identities of any third parties to whom such personal information has been disclosed.[137]

VIII
The European Directive on Data Protection

In contrast to the United States initiatives, several major European countries, such as Germany and the United Kingdom, have already adopted elaborate restrictions on the gathering, use, and transfer of personal data. Such restrictions will apply to personal data

130. H.R. 3508, 104th Cong. (1996).

131. *Id.* A "list broker" is defined as a "person who, in the course of business, provides mailing lists, computerized or telephone reference services, or the like containing personal information of children."

132. *Id.*

133. H.R. 3685, 104th Cong. (1996).

134. *Id.*

135. H.R. 98, 105th Cong. (1997).

136. *Id.*

137. *Id.*

gathered via the Internet. Recently, the European Union adopted a directive on data protection (the "Directive"), which provides a comprehensive framework for all member countries to follow when enacting privacy legislation.[138] These foreign laws, in turn, will affect how U.S. companies gather or treat data concerning foreign nationals.

The Council of the European Union issued the Directive on Data Protection on October 24, 1995. It emphasizes the importance of protecting privacy rights with regard to personal information, and gives member countries three years to enact legislation and regulations to implement its provisions regarding the processing of personal data.[139] Member countries, however, have up to twelve years to comply with certain provisions regarding the manual processing of personal data.[140]

A. Treatment of Personal Data

"Personal data" is broadly defined in the Directive to include all information that relates to an identified or identifiable individual.[141] "Processing" of that data refers to any operation performed on such data, such as collecting, storing, recording, altering, retrieving, organizing or disclosing it.[142] The Directive protects all personal data that is processed by automatic means or which is processed manually but kept in a filing system where such data is "accessible."[143] Specifically, member countries are required to adopt legislation providing that personal data must be: (1) "processed fairly and lawfully;" (2) "collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes;" (3) accurate and complete for the purposes for which it was collected; and (4) kept in a form which identifies the individual for no longer than is necessary for the purposes for which the data was collected.[144] As long as adequate safeguards are provided, the

138. Council Directive 95/46/ED on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281).

139. *Id.*, arts. 1, 32. The Member States subject to the European Convention are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

140. *See id.* ¶69.

141. *Id.* art. 2.

142. *Id.*

143. *Id.* art. 3.

144. *Id.* art. 6. The Directive allows member countries to exclude from the scope of implementing legislation or regulations the processing of personal data gathered in connection

processing of personal data for historic, statistical, or scientific purposes will not be considered incompatible with the Directive.

Moreover, data may only be processed in a limited set of circumstances, including where: (1) the individual "has unambiguously given his consent" to such processing; (2) "processing is necessary for the performance of a contract" to which the individual is or will become a party; (3) the processing is in "compliance with a legal obligation;" or (4) the processing is necessary to protect the "vital interests" of the person to whom the data pertains.[145] The Directive prohibits the processing of personal data revealing personal information such as "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and . . . data concerning health or sex life" unless the individual consents to such processing or one of the other limited exceptions applies.[146]

In addition, before any previously collected personal data can be disclosed to a third party, the individual must be informed of the entity responsible for processing the data (the "Controller") for that third party, the purposes of the data processing, what type of data will be disclosed, and the identity of the recipients of the data.[147] The individual must also be given the right to correct inaccuracies in the data.[148] These steps need not be followed if the processing is for statistical or historical purposes, if such disclosure would be impossible, if disclosure would "involve a disproportionate amount of effort," or if disclosure of the personal data to a third party "is expressly laid down by law."[149] The "disproportionate effort" exception, however, may substantially reduce the disclosure obligations of merchants.

If consent is required for processing or disclosing information, such consent is not valid unless the individual is informed of the identity of the Controller and the intended purpose of the processing.[150] If applicable, the individual must also be informed of (1) the fact that the individual has the right to review and correct his or

---

with state security, defense, public security, important state financial interests (such as taxation), regulatory functions relating to the foregoing, and criminal and ethical investigations. *Id.* art. 3.

145. *Id.* art 7.

146. *Id.* art. 8.

147. *Id.* art. 11.

148. *Id.* art. 12.

149. *Id.* art. 11.

150. *Id.* art. 19.

her personal data, and (2) whether responses to questions seeking personal data are obligatory or voluntary.[151] Member countries must also give individuals the right, in certain circumstances, to object to the processing of data related to the individual.[152] Specifically, the Directive provides that individuals have the right to be made aware of and to object to, free of charge, the processing of personal data for direct marketing purposes.[153]

B. Country Data Protection Authorities

Each member country must assign "one or more public authorities" to monitor industry compliance with the legislation or regulations adopted pursuant to the Directive.[154] Each supervisory authority will have the ability to investigate data processing operations, to regulate such operations (for example, to institute a ban on processing or to order the destruction of data), and the power to institute legal proceedings.[155] Individuals will also have the right to file administrative claims with the supervisory authority, and to appeal the authority's decisions.[156]

In addition, companies must provide the supervisory authority with certain information before engaging in automated data processing operations (*i.e.*, the name and address of the Controller, the types of data processed, the types of recipients to whom the data might be disclosed, proposed transfers of data to third countries, and general descriptions of security measures).[157] Furthermore, processing operations "likely to present specific risks to the rights and freedom" of individuals will be subject to checks before processing can begin.[158]

C. Prohibitions on the Transfer of Data

The Directive has direct implications for companies operating in the United States because the data protection legislation prohibits the transfer of personal data to a third party country unless that country ensures an adequate level of protection for the personal data.[159] The

151. *Id.* art. 10.
152. *Id.* art. 14.
153. *Id.*
154. *Id.* art. 28.
155. *Id.*
156. *Id.*
157. *Id.* arts. 18, 19.
158. *Id.* art. 20.
159. *Id.* art. 25.

adequacy of such protections will be determined in light of the "total circumstances" surrounding such data transfer operations (*e.g.*, national laws, professional rules, and security measures).[160] Given the lack of United States laws providing protection similar in scope to the Directive, however, it may be difficult for European companies to transfer data to the United States.[161] In the absence of such laws, United States companies may need to enter into contracts with European companies that provide greater protection for personal data of European origin. For example, at the insistence of the German data-protection ombudsman, Citibank agreed to respect German data protection legislation when processing credit application forms for German citizens at its credit card centers in Nevada and South Dakota.[162] In addition, Citibank changed its application form so that financial information need only be disclosed when necessary.[163] The German authorities recognize that the growth of the Internet threatens these data protections.[164] The German government released a draft of proposed legislation addressing numerous issues relating to the use of the Internet, including the privacy of personal data.[165] This legislation limits the collection of personal data to the extent necessary to perform the requested services, after which the data must be immediately erased.[166] Strictly interpreted, such a standard would outlaw the use of "cookies."[167]

IX
Conclusion

The increasing capability of computers and telecommunications to obtain and correlate personal information about individuals continues to raise privacy concerns.[168] If not addressed, these concerns could severely hamper the growth of electronic commerce. In the near

160. *Id.*

161. Participants in the FTC's June workshop offered different views of whether existing privacy protections in the United States satisfy the Directive's "adequacy" standard.

162. Gumbel, *supra* note 7, at A6.

163. *Id.*

164. *Id.*

165. Bruno Giussani, *Proposed German Statute Would Regulate Content*, N.Y. TIMES CYBERTIMES (Jan. 11, 1997)<http://search.nytimes.com/web/docsroot/library/cyber/euro/011197euro.html>.

166. *Id.*

167. *Id.*

168. *See, e.g.*, Nina Bernstein, *On Frontier of Cyberspace Data is Money, and a Threat*, N.Y. TIMES, June 12, 1997, at A1, A15-16.

term, industry, privacy advocates, and the United States government will continue to study and debate these issues. Given the policy differences between these groups, it is questionable whether the United States will enact comprehensive privacy legislation in the near future. The enactment of privacy legislation in the European Union, however, may accelerate the adoption of comprehensive privacy laws in the United States.

At present, lawyers should make sure that their clients are aware of these issues. If a client's business is international, it should consider implementing procedures to comply with the European Directive. In implementing such a privacy policy, a company needs to review both United States laws and the European Directive, and should consider the following issues:

- What type of personal information will be collected?
- How long will the personal information be retained?
- For what purposes will the personal information be used?
- How can a consumer indicate a limitation on the use of their personal information (*i.e.*, opt-in, or opt-out)?
- Will the information be purged? If so, at what time?
- Will personal information be provided to third parties and, if so, for what purposes?
- How can a consumer obtain access to his or her personal information and provide corrected information?
- Is the personal information subject to special regulation by the state or federal government (*i.e.*, credit information)?

By developing a policy that addresses these issues, companies can engage in electronic commerce without violating either United States or foreign privacy laws.